REMARKS

The Examiner is thanked for the indication that claims 1-3, 7-12, 15-19, and 21-23 are allowed. Claims 1-3, 7-12, 15-19, and 21-27 remain pending in the instant application. Claims 24-26 presently stand rejected. Claim 27 presently stands objected to. Claims 24 and 27 are amended herein. Entry of this amendment and reconsideration of the pending claims are respectfully requested.

Claim Rejections – 35 U.S.C. § 102

Claims 24-26 stand rejected under 35 U.S.C. § 102(a) as being anticipated by Garfinkel et al., "Terra: A Virtual Machine-Based Platform for Trusted Computing." The rejections are respectfully traversed.

A claim is anticipated only if each and every element of the claim is found in a single reference. M.P.E.P § 2131 (citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the claim." M.P.E.P. § 2131 (citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226 (Fed. Cir. 1989)).

Independent claim 24 as amended recites:

A method, comprising:

loading an untrusted virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer;

loading a first and a second virtual machine (VM) supported by the VMM;

sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer;

receiving a request for a VMM service that is associated with the first VM, wherein the request comprises a challenger hash value;

determining a first VM platform configuration including a first hash value based on information measured from the first VM and a second VM platform configuration including a second hash value based on information measured from the second VM;

using a trusted hardware device shared between the first and the second VM to determine a stored compound hash value based on a combination of the first VM platform configuration and the second VM platform configuration;

computing a current compound hash value based on a combination of the first VM platform configuration including the challenger hash value and the second VM platform configuration including the second VM hash value;

determining whether the current compound hash value is equal to the stored compound hash value; and

executing the received request when the current compound hash value is equal to the stored compound hash value.

Applicants respectfully submit that *Garfinkel* fails to disclose at least the above limitations. In particular, Applicants note that the cited art fails to teach an untrusted VMM. In the Office Action response to arguments, it is submitted that Garfinkel is addressed to hosting multiple VMs on a VMM and, hence, multiple hosted VMs can be attested. However, *Garfinkel* teaches implementing identification of remote parties to trusted VMM to a selected VM (*arguendo*). Because *Garfinkel* is a trusted VMM, *Garfinkel* is directed towards identification between remote parties and a specific, single

VM, and does not motivate, for example, combining attestations from first and second VMs (as discussed below).

Thus, *Garfinkel* does not teach a second VM platform configuration including the second VM hash value because *Garfinkel* teaches attestation solely between a single VM and a single remote party (page 195, right column, fifth full paragraph). The attestation is addressed to a particular piece of software (for which the third party already has a hash value, *see* section 4.3, third paragraph) rather than to a hardware configuration, as recited by the claim. Further, "Receiving an attestation tells the remote party what program was started on a platform, but it does not confirm that the program has not subsequently been compromised" (*see*, section 2.2, first paragraph) Thus the hash values of *Garfinkel* are directed toward specific, known-beforehand software applications, rather than verifying known current hardware configurations of VMs.

Further, claim 24 has been amended to recite (for example) determining a first VM platform configuration including a first hash value based on information measured from the first VM and a second VM platform configuration including a second hash value based on information measured from the second VM. *Garfinkel* does not teach determining a first VM platform configuration including a first hash value based on information measured from the first VM and a second VM platform configuration including a second hash value based on information measured from the second VM.

Consequently, *Garfinkel* fails to disclose each and every element of claim 24, as required under M.P.E.P. § 2131. Accordingly, Applicants request that the instant §102 rejections of claim 24 be withdrawn.

The dependent claims 25, 26, and 27 are novel over the prior art of record for at least the same reasons as discussed above in connection with their respective independent claims, in addition to adding further limitations of their own. Accordingly, Applicants respectfully request that the instant § 102 rejections of the dependent claims be withdrawn.

Claim Objections

Claim 27 stands objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claim 27 is believed to be allowable for at least the reasons stated above with respect to the base claim.

CONCLUSION

In view of the foregoing amendments and remarks, it is believed that the applicable rejections have been overcome and all claims remaining in the application are presently in condition for allowance. Accordingly, favorable consideration and a Notice of Allowance are earnestly solicited. The Examiner is invited to telephone the undersigned representative at (206) 292-8600 if the Examiner believes that an interview might be useful for any reason.

CHARGE DEPOSIT ACCOUNT

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a). Any fees required therefore are hereby authorized to be charged to Deposit Account No. 02-2666. Please credit any overpayment to the same deposit account.

Respectfully submitted,
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Date: July 14, 2008

/Mark Hennings/

Mark R. Hennings
Reg. No. 48,982

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Phone (206) 292-8600

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being transmitted electronically via EFS-Web to The United States Patent and Trademark Office on the date shown below.

/Elizabeth J. Martinez/ July 14, 2008
Elizabeth J. Martinez *Date*